AIR FORCE RESEARCH LABORATORY
ROME, NEW YORK

REVISED
STATEMENT OF SCOPE

FOR

Databases for the 21st Century II (DB21 II):
Information, Intelligence, and Information Warfare (I2/IW)

PR NO. E-2-1205

22 AUG 2001

(Contract No. F30602-01-D-0167)

Attachment No. 2

TABLE OF CONTENTS

PARA	SUBJECT	PAGE
1.0	OBJECTIVE	3
2.0	SCOPE	4
3.0	BACKGROUND	6
4.0	TASKS/TECHNICAL REQUIREMENTS	11
4.1	AFIWC AND DAWS/DMFE/IET: ANNUALLY BASIC RECURRING WORK AND PDL WORK	11
4.2	IDIQ ORDER WORK	20
	ANNEX I AFIWC REQUIREMENTS DOCUMENT (Recurring 3400 Funded Work)	32
	ANNEX II DAWS/DMFE/IET REQUIREMENTS DOCUMENT (Recurring 3400 Funded Work)	44
	ANNEX III AFRL/IFE/IFEA/IFEB/IFEC/IFED TECHNICAL AREAS	53
	ANNEX IV AFRL/IFGB TECHNICAL AREAS	55
	ANNEX V AFIWC TECHNICAL AREAS	56
	ANNEX VI DAWS/DMFE/IET TECHNICAL AREAS	59

1.0 OBJECTIVE: The objective of this effort is to: 1) support the advancement, integration, and application of Information Systems Science and Technology to meet Air Force (AF), Intelligence Community, and Command and Control (C2) Community unique requirements for Information Dominance and 2) facilitate the transition of this technology to aerospace and intelligence systems to meet AF, Intelligence and C2 Community needs.

A primary goal of this effort is to facilitate rapid technology advancement, insertion and integration to meet a wide variety of customer needs, with maximization of systems interoperability through the use of commercial off-the-shelf (COTS)/government off-the-shelf (GOTS) technology, prototyping, and non-proprietary technology. These technology activities are to be accomplished while promoting high quality, timely, and economical solutions to satisfy customer requirements.

Specifically, this effort will provide support to the following organizations and their customers:

1.1 THE AIR FORCE INFORMATION WARFARE CENTER (AFIWC)

The Air Force Information Warfare Center (AFIWC), a collocated unit of the Air Intelligence Agency, Kelly Air Force Base, Texas.

1.2 AFRL/IFEB'S DEFENSE AUTOMATED WARNING SYSTEM (DAWS)/ MESSAGE FRONT END (DMFE)/INFORMATION EXTRACTION TOOL (IET) PROGRAM

The Air Force Research Laboratory (AFRL), Information Handling Branch's (IFEB) Defense Automated Warning System (DAWS)/Message Front End (DMFE)/Information Extraction Tool (IET) Program.

1.3 THE AFRL INFORMATION & INTELLIGENCE EXPLOITATION DIVISION (IFE)

The Information and Intelligence Exploitation Division (IFE) of the Air Force Research Laboratory (AFRL), Information Directorate (IF) at Rome NY, including its Fusion Technology Branch (IFEA), Information Handling Branch (IFEB), Multi-Sensor Exploitation Branch (IFEC), and Global Information Base Branch (IFED).

1.4 AFRL DEFENSIVE INFORMATION WARFARE BRANCH (IFGB)

The Defensive Information Warfare Branch (IFGB) of the Air Force Research Laboratory (AFRL), Information Directorate (IF) at Rome NY.

2.0 SCOPE:

The work performed under this effort will span the spectrum from Basic Research to Operations and Maintenance (O&M) activities. The work may include, but shall not be limited to: analytical studies, system feasibility studies, system design, engineering efforts, system trade-off studies, experimental design efforts, experimental hardware/software demonstration efforts, software specification efforts, software development efforts, system simulations, component and systems integration, test and evaluation analyses, advanced system developments and advanced hardware component development efforts, rapid prototyping, and system analyses.

2.1 SUPPORT FOR AFIWC AND DAWS/DMFE/IET ANNUALLY RECURRING O&M ACTIVITIES AND GENERAL REQUIREMENTS (LEVEL-OF-EFFORT (LOE)/PDLs)

2.1.1 AFIWC

Provide LOE Support for the information architecture requirements of the Air Force Information Warfare Center (AFIWC), to properly accomplish its mission. This will include defined, annually recurring O&M activities (see paragraph 4.1) on a Government

Fiscal Year (GFY) basis and general requirements (see Annex I) that will be defined via Performance Details Letters (PDLs) and issued to the contractor for execution on an as-needed basis. This work shall be conducted for each contractually covered Government Fiscal Year (GFY) or portion thereof, at the discretion of the Government. Effort will be conducted on a GFY option basis designated by the Contracting Officer.

2.1.2 DAWS/DMFE/IET

Supporting the information architecture requirements of AFRL/IFEB's Defense Automated Warning System (DAWS)/Message Front End (DMFE)/Information Extraction Tool (IET) Program. This will include defined, recurring O&M activities (see paragraph 4.2) on a Government Fiscal Year (GFY) basis and general requirements (see Annex II) that will be defined via Performance Details Letters (PDLs) and issued to the contractor for execution on an as-needed basis. This work shall be conducted for each contractually covered Government Fiscal Year (GFY) or portion thereof, at the discretion of the Government. Effort will be conducted on a GFY option basis designated by the Contracting Officer.

2.2 WORK FOR IFE, IFGB, AFIWC, AND DAWS/DMFE/IET (COMPLETION, IDIQ ORDERS)

The scope of this effort includes the technology areas in ANNEX III for the IFE Division and those of the IFGB Branch, identified in ANNEX IV, as well as related technologies and those of their customers. It also includes AFIWC and DAWS/DMFE/IET requirements (see ANNEXES V and VI)for specific deliverable end items. The effort includes: analytical studies, system feasibility studies, system design, engineering efforts, system trade-off studies, experimental design efforts, experimental hardware/software demonstration efforts, software specification efforts, software development efforts, system simulations, component and systems integration, test and evaluation analysis, advanced system developments and advanced hardware component development efforts, rapid prototyping, and system analyses. Full spectrum system design efforts will be conducted on an order basis designated by the Contracting Officer.

2.3 IFE, IFGB, AFIWC, AND DAWS/DMFE/IET CUSTOMERS:

Supporting requirements including, but not limited to AFRL/IF; AFIWC; DAWS/DMFE/IET; the Air Force and other Services; DOD; Unified Commands; Intelligence and Command and Control (C2) Communities; General Military Intelligence (GMI) Community; National Migration Systems; Air Force Material Command (AFMC); the warfighter; the AS2IRC; and Air Force, DOD and National Command, Control, Communications and Intelligence (C3I) systems.

3.0 BACKGROUND:

3.1 THE AIR FORCE INFORMATION WARFARE CENTER (AFIWC)

The Air Force Information Warfare Center, collocated with the Air Intelligence Agency, was created to be an information superiority center of excellence, dedicated to offensive and defensive counter information and information operations. AFIWC was originally activated as the 6901st Special Communication Center in July 1953. The following month, the 6901st was re-designated as the Air Force Special Communication Center. It was then re-designated as the Air Force Electronic Warfare Center (AFEWC) in 1975.

Air Force successes in exploiting enemy information systems during Operation Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare. In response, the AFIWC was activated Sept. 10, 1993, combining technical skills from the former AFEWC, the Air Force Cryptologic Support Center's Securities Directorate, and intelligence skills from the former Air Force Intelligence Command.

AFIWC's team of more than 1,200 military and civilian members is skilled in the areas of operations, engineering, operations research, intelligence, radar technology, communications and computer applications. The members are dedicated to providing

improved command and control warfare and information warfare (IW) capabilities to the warfighting U.S. Air Force major commands.

3.1.1 AFIWC MISSION

The mission of the AFIWC is to explore, apply, and migrate offensive and defensive information warfare capabilities for operations, acquisition and testing, and provide advanced information warfare training for the Air Force.

3.1.2 AFIWC VISION

The vision of the AFIWC is to be the premier organization for integrating information warfare across the full spectrum of Air Force operations.

3.1.3 AFIWC GOALS

- Develop and demonstrate operationally relevant and innovative IW concepts and technologies
- Transfer IW knowledge, capabilities, and expertise to strategic and tactical operations
- Improve our capability to conduct IW analysis, mission planning, and tactics evaluation and development
- Develop an advanced IW training capability
- Develop a standardized, state-of-the-art communications structure linking internal and external customers
- Implement a center-wide internal training program

The AFIWC is engaged in a myriad of activities supporting its role as the Air Force information warfare executive agent. The center provides information warfare services to the warfighter in contingencies and exercises through quantitative analysis, modeling and simulation, database and technical expertise in communication and computer security. The

reputation of the AFIWC as the premier DOD IW organization is reflected through the outstanding performance of a diverse mission base.

3.2 THE DEFENSE AUTOMATED WARNING SYSTEM (DAWS)/MESSAGE FRONT END (DMFE)/INFORMATION EXTRACTION TOOL (IET) PROGRAM PROGRAM

DAWS/DMFE/IET is AFRL's tool for providing the intelligence analyst with value-added message profiling, retrospective search and message generation capabilities to supplement the Defense Message System (DMS). It is a potential replacement for the legacy DODIIS Automated Message Handling System (AHMS). DAWS/DMFE/IET interfaces with CSP/CDAC and is able to store and search both organizational message traffic and email messages with enclosures, facilitating DODIIS Community transition to the SCI DMS architecture.

3.3 THE INFORMATION & INTELLIGENCE EXPLOITATION DIVISION (IFE)

The mission of the Information and Intelligence Exploitation Division is to conduct research and development to implement Global Awareness and support Precision Engagement and Full Dimensional Aerospace Protection by advancing the state of the art in intelligence and surveillance and reconnaissance exploitation capabilities. Technologies developed support collection, processing, storage, fusion, and dissemination of both real-time and stored information in support of all battlespace participants. The division partners with the Sensor ATR Division of the Sensors Directorate and relies on them to develop the sensor ATR technology to detect, track and ID targets for inputs into the Global Awareness picture. The Division conducts selected acquisition programs for low-volume, limited quantity systems for the intelligence community.

IFE Technologies:

- Fusion Technology Branch (IFEA)
- Information Handling Branch (IFEB)

- Multi-Sensor Exploitation Branch (IFEC)
- Global Information Base Branch (IFED)

3.3.1 FUSION TECHNOLOGY BRANCH (IFEA)

Identifies and develops technologies so that real-time and stored data are fused to support global awareness. Integrates technologies to provide a common operating picture to dynamic planning and to the data warehouse functions. Provides feedback to the data collection operation to improve quality of targeting. The Sensor ATR Division will develop the sensor ATR technology to detect, track and ID targets for inputs into the fused global awareness picture. Develops capabilities to differentiate potential targets as friend, foe, or neutral sufficient time, with high confidence and at the requisite range to support weapons release and engagement decisions.

3.3.2 INFORMATION HANDLING BRANCH (IFEB)

Identifies, develops, prototypes, transitions and supports advanced technologies and approaches to the acquisition, analysis, and timely dissemination of intelligence information for the Intelligence Community. These techniques will acquire and assimilate disseminate intelligence products needed by decision makers and warfighters to ensure battlespace dominance.

3.3.3 MULTI-SENSOR EXPLOITATION BRANCH (IFEC)

Advance the state-of-the-art in multi-sensor imagery and signals intelligence exploitation technologies. Cost-effectively transition these technologies to Air Force, DOD and National Command, Control, Communications and Intelligence (C31) systems to ensure the sustainment of an information-dominant fighting force.

3.3.4 GLOBAL INFORMATION BASE BRANCH (IFED)

Conducts research in information management, storage and retrieval, to provide a full suite of access services for "on-time" C4I information to the warfighter. Techniques for comprehensive knowledge of the battlespace are developed so that all warfighters, from the theater Commander to each individual combatant has the proper information to support their decisions and actions.

3.3.5 DEFENSIVE INFORMATION WARFARE BRANCH (IFGB)

Supports the full spectrum of Air Force information operations from peace time through crises and war and back to peace. Applies information technology across the spectrum of information operations in support of Air Force mission requirements. Provides research and development in the areas of computer and network risk assessment and management, security services for assurance, vulnerability analysis, detection of intrusions and misuse, and assessment of information damage; and recovery of data and systems to operational levels.

4.0 TASKS/TECHNICAL REQUIREMENTS:

4.1 AFIWC AND DAWS/DMFE/IET: ANNUALLY BASIC RECURRING WORK AND PDL WORK

For all work to be performed, the contractor shall provide flexible technical, managerial, contracting/subcontracting and business processes, compatible with the volatile nature of the defense industry and the political and operating environment in which the AFIWC, the DAWS/DMFE/IET Program and their customers function.

4.1.1 AFIWC WORK

The contractor shall accomplish the following activities levied against the AFIWC basic recurring requirements identified in Annex I. Activities are defined as the following: Software development, Software development methods, Standards for software products, Reusable software products, Handling of critical requirements of Safety assurance, Security assurance and Privacy assurance, Computer hardware resource utilization, Project planning and oversight, Establishing a software development environment, System requirements analysis, System design, Software requirements analysis, Software design, Software implementation and unit testing, qualification testing, integration and testing, System qualification testing, Preparing for software use, Preparing version descriptions for user sites, Preparing user manuals, Installation at user sites, software transition, Software configuration management, Software product evaluation, Software quality assurance, Corrective action and system maintenance and Joint technical and management reviews. (see CDRL)

In addition, the contractor shall accomplish the above activities further defined via PDLs levied against the AFIWC requirements identified in Annex I. All official PDLs will be issued by the AFRL DB21 II Contracting Officer only.

4.1.2 DAWS/DMFE/IET WORK

The contractor shall accomplish the following activities levied against the DAWS/DMFE/IET recurring requirements identified in Annex II. Activities are defined as the following: Software development, Software development methods, Standards for software products, Reusable software products, Handling of critical requirements of Safety assurance, Security assurance and Privacy assurance, Computer hardware resource utilization, Project planning and oversight, Establishing a software development environment, System requirements analysis, System design, Software requirements analysis, Software design, Software implementation and unit testing, qualification testing, integration and testing, System qualification testing, Preparing for software use, Preparing version descriptions for user sites, Preparing user manuals, Installation at user sites, software transition, Software configuration management, Software product evaluation, Software quality assurance, Corrective action and system maintenance and Joint technical and management reviews.(see CDRL)

In addition, the contractor shall accomplish the above activities further defined via PDLs levied against the DAWS/DMFE/IET requirements identified in Annex II. All official PDLs will be issued by the AFRL DB21 II Contracting Officer only.

4.1.3 MANAGEMENT OF AFIWC AND DAWS/DMFE/IET WORK

4.1.3.1 Provide flexible management, contracting/subcontracting, business and technical processes compatible with the volatile nature of the defense industry including the political and operating environment in which the AFIWC, the DAWS/DMFE/IET Program and their customers function.

4.1.3.2 Program Management

Plan, organize, and manage the resources necessary to accomplish the contract requirements.

4.1.3.3 Manage program cost, schedule, performance, risks, contracts and subcontracts, problems, data, and warranties required to deliver technically acceptable, and cost-effective work, deliverables, and products. Allow and maintain government visibility into overall contract and individual PDL costs, schedules, technical performance, risk management, problems and problem resolution. These management activities shall also include, but not be limited to: (see CDRL)

- Costs
- Schedules
- Performance
- Risk Management
- Problems and problem resolution
- Security and DD254s
- Billets
- Government Furnished Property (GFP)
- Government Furnished Information (GFI)
- Contractor Acquired Property (CAP)
- Deliverables and DD250s

4.1.3.4 Execution Plans.

The contractor shall prepare separate execution plans for GFY recurring basic work for both AFIWC and IET, for Government approval. The execution plan shall consist of, but not be limited to, identification and description of the following: the work to be performed; schedules; budgets; estimated expenditures; resources; ODC's; travel; GFP/GFI/Base Support; contractor acquired property (CAP); special requirements; dependencies; risks and risk mitigation plans; security requirements; billet requirements. The execution plan shall be updated and provided to the Government quarterly or as needed. Each update shall clearly identify changes from the previous submission. (see CDRL)

4.1.3.5 Risk Management

During the development process, provide risk management, assessments, reviews, and audits.

4.1.3.6 Management Overview Information for the IFE DB21 II Program Manager (PM), the AFIWC DB21 II PM, and the DAWS/DMFE/IET PM.

Provide the IFE Program Manager (PM) for the DB21 II: I2/IW contract, with overview management information pertaining to all of the work being exercised under the entire AFIWC and DAWS/DMFE/IET recurring and PDL work contract, on a monthly basis, with updates as requested. This information shall be broken out for both AFIWC and DAWS/DMFE/IET as well as by recurring and PDL work. An overall contract summary combining the AFIWC and DAWS/DMFE/IET information shall also be provided for appropriate information such as cost and LOE expenditures. Separate copies of the applicable portion of this information will also be provided to the AFIWC DB21 II PM and the AFRL/IFEB DAWS/DMFE/IET PM, respectively. Sample management information will consist of, but not be limited to, the following: (see CDRL)

- Total dollar amount under contract .
- Dollar amount of work by effort (recurring/PDL) under contract, including unfunded amounts, estimates at completion, projected cost under/over-runs.
- Expenditure rate of dollars, labor, materials, travel and other charges by recurring/PDL work. Impact of deviations, resolution.
- Contractor responsible for the work, recurring/PDL.
- Description of work performed including work status and an estimate of percentage of work completed.
- Schedule status information including planned vs. actual, milestones.

- Problems/difficulties encountered, including impact on work. Problem resolution and schedule of solution.
- Progress of work.
- Work plans for the next reporting period.

4.1.3.7 Management Overview Information for PDL Managers On Individual PDLs.

Provide each PDL Program Manager (PM) separate overview management information pertaining to their specific PDL being exercised under the contract, monthly, or as required in the PDL, with updates as requested. Sample PDL management information will consist of, but not be limited to, the following: (see CDRL)

- Total Dollar Amount of the PDL under Contract (including options if any).
- Expenditure Rate of Dollars by PDL, for labor, materials, travel and other PDL charges, impact of deviations, resolution.
- Contractor responsible for the PDL
- Description of work performed including work status and an estimate of percentage of work completed.
- Schedule status information including planned vs. actual, milestones.
- Problems/difficulties encountered on the PDL, impact on PDL, problem resolution.
- Work plans for the next reporting period.

4.1.3.8 Conduct Oral Presentations/Reviews/Meetings at such times and places as designated in the Contract Schedule or as agreed to by both the Government and the contractor. (see CDRL)

4.1.3.9 Perform the following management activities:

- Risk management

- Software management indicators
- Security and privacy
- Subcontractor management
- Interface with software IV&V agents
- Coordination with associate developers, Government organizations and their customers
- Improvement of project technical, management, contracting, and business processes

4.1.3.10 Support unexpected and quick reaction requirements.

4.1.3.11 Utilize Integrated Products and Processes in the analysis, design, development, test and management/business/contracting/subcontracting processes. Ensure a team atmosphere with the government, their customers, and other contractor team members, subcontractors, associate contractors and consultants.

4.1.3.12 Incorporate the functional areas of systems engineering, engineering data and specifications, software development, configuration management, quality assurance, integrated logistics support, financial management, and specialty engineering into a single Integrated Master Schedule (IMS) for both the AFIWC and DAWS/DMFE/IET work.(see CDRL)

4.1.3.13 Utilize appropriate reviews to inform the Government of progress/status.

4.1.3.14 Utilize Contractor/Government (IFE-AFIWC-DAWS/DMFE/IET)/Customer document/data sharing by compatible, on-line electronic means that minimize man-in-the-loop conversion actions.

4.1.3.15 Establish and maintain a risk management program encompassing the areas of risk planning, assessment, analysis, and handling. Promote a risk reduction process that minimizes cost and schedule impact and describes a simple, but complete method of

surveying individual potential risks and identifying the degree or level of risk at each system level.

4.1.4 FAMILIARIZATION

Provide on-site familiarization for the developed products, software applications and tools under the recurring work and PDLs, to AFIWC, DAWS/DMFE/IET and AFRL/IF personnel as applicable. This shall include familiarization associated with testing, as well as procedures for maintaining software and systems.(see CDRL)

4.1.5 TESTING

4.1.5.1 Conduct Test and Evaluation Analysis that include the analysis of field or operational tests of advanced systems.

4.1.5.2 Perform software implementation and unit testing, qualification testing, integration and testing, system qualification testing, system Security testing, JITF testing, and DMB required testing as required.(see CDRL)

4.1.6 DOCUMENTAION

The following shall apply to all work performed under the DB21 II: I2/IW contract unless specified otherwise in individual PDLs or execution plans:

4.1.6.1 Continually determine the status of the effort and report progress toward accomplishment of contract requirements.(see CDRL)

4.1.6.2 Continually determine the status of funding required for contract performance.(see CDRL)

4.1.6.3 Continually update and maintain an Integrated Master Schedule for both AFIWC and DAWS/DMFE/IET work. (see CDRL)

4.1.6.4 Document all technical work accomplished and information gained during performance of this acquisition. Include all pertinent observations, nature of problems, positive and negative results, and design criteria established where applicable. Document procedures followed, processes developed, "Lessons Learned," etc. Document the details of all technical work to permit full understanding of the techniques and procedures used in evolving technology or processes developed. Cross-reference separate design, engineering, or process specifications delivered to permit a full understanding of the total acquisition. (see CDRL)

4.1.6.5 Conduct oral presentations at such times and places designated in the contract schedule. Provide status of technical progress made to date in performance of the contract during presentations.(see CDRL)

4.1.6.6 Update the existing Government Furnished Documentation in the form of revisions, which clearly identify the update. Format and content of the changes shall not deviate from that of the existing documentation. (see CDRL)

4.1.7 SOFTWARE

The following shall apply to all work performed under the DB21 II: I2/IW contract unless specified otherwise in individual PDLs or execution plans:

4.1.7.1 Develop all software using best commercial practices. Design and develop all computer software using an approved Higher Order Language (HOL). Submit the choice of HOL to the Government and provide justification for the HOL selected. Document the selection criteria based upon system interface, interoperability, communications functions, human interface and requirements for security, safety and reliability.

4.1.7.2 Deliver all computer software developed, assembled, or acquired to the Government in accordance with the Contract schedule and the following:

4.1.7.2.l Deliver all computer software developed under this effort to the Government in the form of source and object (executable) code. (see CDRL)

4.1.7.2.2 Deliver all software assembled or acquired under this effort to the Government in the form of object (executable) code only.

4.1.7.3 Document all software in the form of hard copies and electronic media in accordance with the Contract Data Requirements List (CDRL) and the requirements of each PDL. (see CDRL)

4.1.7.4 Delivered software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation.

4.1.7.5 Evaluate and plan for the use of Non-Developmental (Commercial Off-the-Shelf (COTS), Reusable, Government Furnished) Software as applicable, to ensure that all SOW and PDL requirements have been met. Upon acquisition, evaluate the software to determine whether it performs as documented and prior to incorporating it into the software being developed. Certify that the Non-Developmental Software performs as documented and is documented adequately.

4.1.7.6 For all software purchased or licensed for use as a component of the software to be delivered, arrangements shall be made for licensing and maintenance agreements to be transferred to the Government upon the completion of this effort. (see CDRL)

4.1.7.7 All information technology items must be year 2000 compliant, or non-compliant items must be upgraded at no additional cost to be year 2000 compliant upon delivery. Year 2000 compliant means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and

between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.

4.1.7.8 Provide complete identification, tracking , and control of system software, hardware, and interfaces. Provide assurance that the system meets the specifications and requirements for its intended use and performance.

4.1.7.9 The Air Force Computer Emergency Response Team (AFCERT), established by AFR 205-16, issues advisories to identify known vulnerabilities in computers and computer networks. These advisories include but are not limited to Information Assurance Vulnerability Alerts, Virus notification, Advisory Compliance Messages (ACMs), and Follow-Up Messages. The Contractor shall report suspected vulnerabilities and security incidents in accordance with AFSSI 5021. The Contractor shall respond to AFCERT advisories in accordance with AFSSI 5021 as follows:

4.1.7.9.1. Acknowledge receipt of AFCERT advisories in three (3) days of issue.

4.1.7.9.2. Implement the countermeasures identified by the advisory within the timeframe specified by the advisory or as specified by the Government, AFIWC, the DAWS/DMFE/IET Program or the customer/requiring activity. If the countermeasures cannot be implemented, the Contractor shall document the inability and must receive approval from the Designated Approving Authority (see AFI 33-202) and the Government, AFIWC, the DAWS/DMFE/IET Program or the customer/requiring activity as applicable, for either an alternative corrective action or to continue operations without the countermeasures. If alternative corrective action is approved, the Contractor shall implement this action within the timeframe specified by the Government, AFIWC, the DAWS/DMFE/IET Program or the customer/requiring activity.

4.2 WORK FOR IFE, IFGB, AFIWC, AND DAWS/DMFE/IET (COMPLETION, IDIQ ORDERS)

For all work to be performed, the contractor shall provide flexible technical, managerial, contracting/subcontracting and business processes, compatible with the volatile nature of the defense industry and the political and operating environment in which IFE, IFGB, AFIWC, DAWS/DMFE/IET and their customers function.

The contractor shall accomplish the following activities as required in accordance with the requirements in Annexes III, IV, V, and VI and the individual Order Requirements for IFE, including all of its Branches; IFGB; the AFIWC; the DAWS/DMFE/IET Program, and their customers:

4.2.1 Perform analytical studies, feasibility analysis, system design studies, system trade-off studies, prototype design efforts, software specification efforts, software development efforts, system simulation, component and system integration, test and evaluation analysis, system developments and hardware component development efforts. The specific support required for each Order will be identified in an Order Requirement issued by the DB21 II Contracting Officer. (see CDRL)

4.2.1.1 Conduct Analytical Studies to include technical evaluation of engineering problem areas and development of solutions to these problems.

4.2.1.2 Conduct Analytical Studies to include technical evaluation of engineering problem areas and development of solutions to these problems.

4.2.1.3 Conduct System Feasibility Studies that include requirement definition and cost performance analysis.

4.2.1.4 Develop System Designs that result in a recommended system specification for an advanced system model.

4.2.1.5 Conduct System Trade-Off Studies that evaluate multiple solutions to problems and results in recommendations of the most technical and cost-effective solutions.

4.2.1.6 Develop Prototype Designs that recommend the most appropriate methodology required to verify the results of a prior analytical study.

4.2.1.7 Develop Prototype Hardware/Software Demonstrations, acquire, assemble, and integrate all hardware and software required to conduct verification/validation of the analytical study.

4.2.1.8 Develop Software Specifications.

4.2.1.8.1 Develop Software Specifications by analyzing the results of a demonstration effort or the results of a system requirement definition.

4.2.1.8.2 Develop the algorithm and detailed software specifications for solutions to the problem of interest.

4.2.1.8.3 Design the solutions to work in an operational environment.

4.2.1.9 Develop software that includes code development and documentation of operational software.

4.2.1.10 Develop System Simulations that include computer simulations, hardware simulations, and hybrids thereof.

4.2.1.11 Conduct Test and Evaluation Analysis that include the analysis of field or operational tests of advanced systems.

4.2.1.12 Determine Life Cycle Costing requirements.

4.2.1.13 Determine Design-To-Cost requirements.

4.2.1.14 Conduct a Reliability and Maintainability Program.

4.2.1.15 Conduct a Logistics Support Program.

4.2.1.16 Conduct a Configuration Management and Quality Assurance Program.

4.2.1.17 Conduct on-site assessments of operational systems or class of systems to identify problem areas and recommend solutions.

4.2.1.18 Conduct Oral Presentations/Reviews/Meetings at such times and places as designated in the Contract and Order Schedule. (see CDRL)

4.2.1.19 Familiarization. Provide on-site familiarization of the developed software applications and tools to AFRL/IF, AFRL/IFE, AFRL/IFGB, AFIWC, and DAWS/DMFE/IET personnel and their customers, as applicable, associated with testing under the tasks as well as procedures for maintaining software.(see CDRL)

4.2.1.20 Configuration Management. Implement a process for managing the development and integration of the deliverable software. The software development process shall include the following activities: System Requirements Analysis/Design, Software Requirements Analysis, Preliminary Design, Detailed Design, Coding and Computer Software Configuration Item Testing, and System Integration and Testing. Participate in design reviews conducted by the Government for other development efforts that may impact this effort.

4.2.1.21 Risk Management. During the software development process, provide risk management, assessments, reviews, and audits.

4.2.1.22 Program Management. Plan, organize, and manage the resources necessary to accomplish the contract/order requirements.

4.2. 2 MANAGEMENT

4.2.2.1 Provide flexible management, contracting/subcontracting, business and technical processes, compatible with the volatile nature of the defense industry including the political and operating environment in which the IFE, IFGB, AFIWC, the DAWS/DMFE/IET Program and their customers function.

4.2.2.2 Program Management

Plan, organize, and manage the resources necessary to accomplish the contract requirements.

4.2.2.3 Manage program cost, schedule, performance, risks, contracts and subcontracts, problems, data, and warranties required to deliver technically acceptable, and cost effective work, deliverables, and products. Allow and maintain government visibility into overall contract and individual order costs, schedules, technical performance, risk management, problems and problem resolution. These management activities shall also include, but not be limited to: (see CDRL)

- Costs
- Schedules
- Performance
- Risk Management
- Problems and problem resolution
- Security and DD254s
- Billets
- Government Furnished Property (GFP)
- Government Furnished Information (GFI)
- Contractor Acquired Property (CAP)

- Deliverables and DD250s

4.2.2.4 Risk Management

During the development process, provide risk management, assessments, reviews, and audits.

4.2.2.5 Management Overview Information for the IFE DB21 II PM, the AFIWC DB21 II PM, and the DAWS/DMFE/IET PM

Provide the IFE Program Manager (PM) for the DB21 II: I2/IW contract, with overview management information pertaining to all of the work being exercised under the entire IDIQ contract, on a monthly basis, with updates as requested. This information shall be broken out by primary customer: IFE, IFGB, AFIWC and DAWS/DMFE/IET etc. An overall contract summary combining all of the above information shall also be provided for appropriate information such as cost and LOE expenditures. Separate copies of the applicable portion of this information will also be provided to the AFIWC DB21 II PM and the AFRL/IFEB DAWS/DMFE/IET PM, respectively. Sample management information will consist of, but not be limited to, the following: (see CDRL)

- Total dollar amount under contract .

- Organization the work is being performed for including POC information.

- Dollar amount of work by Order under contract, including unfunded amounts, estimates at completion, projected cost under/over-runs.

- Expenditure rate of dollars, labor, materials, travel and other charges by Order. Impact of deviations, resolution.

- Contractor responsible for the work.

- Description of work performed including work status and an estimate of percentage of work completed.
- Schedule status information including planned vs. actual, milestones.
- Problems/difficulties encountered, including impact on work. Problem resolution and schedule of solution.
- Progress of work.
- Work plans for the next reporting period.

4.2.2.6 Management Overview Information for Order PMs on Individual Orders.

Provide each Order Program Manager (PM) separate overview management information pertaining to their specific Order being exercised under the contract, monthly, or as required in the Order, with updates as requested. Sample Order management information will consist of, but not be limited to, the following: (see CDRL)

- Total Dollar Amount of the Order under Contract (including options if any).
- Expenditure Rate of Dollars for labor, materials, travel and other PDL charges, impact of deviations, resolution.
- Contractor responsible for the Order
- Description of work performed including work status and an estimate of percentage of work completed.
- Schedule status information including planned vs. actual, milestones.
- Problems/difficulties encountered on the Order, impact on Order, problem resolution.
- Work plans for the next reporting period.

4.2.2.7 Conduct Oral Presentations/Reviews/Meetings at such times and places as designated in the Contract Schedule or as agreed to by both the Government and the contractor. (see CDRL)

4.2.2.8 Perform the following management activities:

- Risk management
- Software management indicators
- Security and privacy
- Subcontractor management
- Interface with software IV&V agents
- Coordination with associate developers
- Improvement of project technical, management, contracting, and business processes

4.2.2.9 Support unexpected and quick reaction requirements.

4.2.2.10 Utilize Integrated Contractor/Government (IFE-IFGB-AFIWC-DAWS/DMFE/IET)/Customer document/data sharing by compatible, on-line electronic means that minimize man-in-the-loop conversion actions.

4.2.2.11 Establish and maintain a risk management program encompassing the areas of risk planning, assessment, analysis, and handling. Promote a risk reduction process that minimizes cost and schedule impact and describes a simple, but complete method of surveying individual potential risks and identifying the degree or level of risk at each system level.

4.2.3 FAMILIARIZATION

Provide on-site familiarization for the developed products, software applications and tools under each Order, to AFIWC, DAWS/DMFE/IET, AFRL/IF, AFRL/IFE and AFRL/IFGB personnel as applicable. This shall include familiarization associated with testing, as well for procedures for maintaining software and systems. (see CDRL)

4.2.4 TESTING

4.2.4.1 Conduct Test and Evaluation Analysis that include the analysis of field or operational tests of advanced systems.

4.2.4.2 Perform software implementation and unit testing, qualification testing, integration and testing, system qualification testing, system Security testing, JITF testing, and DMB required testing as required. (see CDRL)

4.2.5 DOCUMENTAION

The following shall apply to all work performed under the DB21 II: I2/IW contract unless specified otherwise in individual Orders:

4.2.5.1 Continually determine the status of the effort and report progress toward accomplishment of contract requirements. (see CDRL)

4.2.5.2 Continually determine the status of funding required for contract performance.(see CDRL)

4.2.5.3 Continually update and maintain an Integrated Master Schedule for both AFIWC and DAWS/DMFE/IET work. (see CDRL)

4.2.5.4 Document all technical work accomplished and information gained during performance of this acquisition. Include all pertinent observations, nature of problems, positive and negative results, and design criteria established where applicable. Document procedures followed, processes developed, “Lessons Learned,” etc. Document the details of all technical work to permit full understanding of the techniques and procedures used in evolving technology or processes developed. Cross-reference separate design, engineering, or process specifications delivered to permit a full understanding of the total acquisition. (see CDRL)

4.2.5.5 Conduct oral presentations at such times and places designated in the Order or contract schedule. Provide status of technical progress made to date in performance of the contract during presentations. (see CDRL)

4.2.5.6 Update the existing Government Furnished Documentation in the form of revisions, which clearly identify the update. Format and content of the changes shall not deviate from that of the existing documentation.(see CDRL)

4.2.6 SOFTWARE

The following shall apply to all work performed under the DB21 II: I2/IW contract unless specified otherwise in individual Orders:

4.2.6.1 Develop all software using best commercial practices. Design and develop all computer software using an approved Higher Order Language (HOL). Submit the choice of HOL to the Government and provide justification for the HOL selected. Document selection criteria based upon system interface, interoperability, communication functions, human interface and requirements security, safety and reliability.

4.2.6.2 Deliver all computer software developed, assembled, or acquired to the Government in accordance with the Contract schedule and the following:

4.2.6.3 Deliver all computer software developed under this effort to the Government in the form of source and object (executable) code. (see CDRL)

4.2.6.4 Deliver all software assembled or acquired under this effort to the Government in the form of object (executable) code only.

4.2.6.5 Document all software in the form of hard copies and electronic media in accordance with the Contract Data Requirements List (CDRL) and the requirements of each Order. (see CDRL)

4.2.6.6 Delivered software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation. (see CDRL)

4.2.6.7 Evaluate and plan for the use of Non-Developmental (Commercial Off-the-Shelf (COTS), Reusable, Government Furnished) Software as applicable, to ensure that all SOW and PDL requirements have been met. Upon acquisition, evaluate the software to determine whether it performs as documented and prior to incorporating it into the software being developed. Certify that the Non-Developmental Software performs as documented and is documented adequately.

4.2.6.8 For all software purchased or licensed for use as a component of the software to be delivered, arrangements shall be made for licensing and maintenance agreements to be transferred to the Government upon the completion of this effort. (see CDRL)

4.2.6.9 All information technology items must be year 2000 compliant, or non-compliant items must be upgraded at no additional cost to be year 2000 compliant upon delivery. Year 2000 compliant means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.

4.2.6.10 Provide complete identification, tracking, and control of system software, hardware, and interfaces. Provide assurance that the system meets the specifications and requirements for its intended use and performance.

4.2.6.11 The Air Force Computer Emergency Response Team (AFCERT), established by AFR 205-16, issues advisories to identify known vulnerabilities in computers and computer networks. These advisories include but are not limited to Information Assurance Vulnerability Alerts, Virus notification, Advisory Compliance Messages (ACMs), and Follow-Up Messages. The Contractor shall report suspected vulnerabilities and security incidents in accordance with AFSSI 5021. The Contractor shall respond to AFCERT advisories in accordance with AFSSI 5021 as follows:

4.2.6.11.1 Acknowledge receipt of AFCERT advisories in three (3) days of issue.

4.2.6.11.2 Implement the countermeasures identified by the advisory within the timeframe specified by the advisory or as specified by the Government Order PM or the customer/requiring activity. If the countermeasures cannot be implemented, the Contractor shall document the inability and must receive approval from the Designated Approving Authority (see AFI 33-202) and by the Government Order PM or the customer/requiring activity as applicable, for either an alternative corrective action or to continue operations without the countermeasures. If alternative corrective action is approved, the Contractor shall implement this action within the timeframe specified by the Government Order PM or the customer/requiring activity.

Databases for the 21st Century II (DB21 II):

Information, Intelligence, and Information Warfare (I2/IW)

ANNEX I:

AFIWC REQUIREMENTS DOCUMENT

FOR

AFIWC GENERAL REQUIREMENTS

1.0 **BACKGROUND INFORMATION**

1.1 AFIWC OVERVIEW

The Air Force Information Warfare Center, collocated with the Air Intelligence Agency, was created to be an information superiority center of excellence, dedicated to offensive and defensive counter information and information operations. AFIWC was originally activated as the 6901st Special Communication Center in July 1953. The following month, the 6901st was re-designated as the Air Force Special Communication Center. It was then re-designated as the Air Force Electronic Warfare Center in 1975.

Air Force successes in exploiting enemy information systems during Operation Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare. In response, the AFIWC was activated Sept. 10, 1993, combining technical skills from the former AFEWC, the Air Force Cryptologic Support Center's Securities Directorate, and intelligence skills from the former Air Force Intelligence Command.

AFIWC's team of more than 1,200 military and civilian members is skilled in the areas of operations, engineering, operations research, intelligence, radar technology, communications and computer applications. The members are dedicated to providing improved command and control warfare and information warfare capabilities to the warfighting U.S. Air Force major commands.

1.2 AFIWC MISSION

The mission of the AFIWC is to explore, apply, and migrate offensive and defensive information warfare capabilities for operations, acquisition and testing, and provide advanced information warfare training for the Air Force.

1.3 AFIWC VISION

The vision of the AFIWC is to be the premier organization for integrating information warfare across the full spectrum of Air Force operations.

1.4 AFIWC GOALS

- Develop and demonstrate operationally relevant and innovative IW concepts and technologies
- Transfer IW knowledge, capabilities, and expertise to strategic and tactical operations
- Improve our capability to conduct IW analysis, mission planning, and tactics evaluation and development
- Develop an advanced IW training capability
- Develop a standardized, state-of-the-art communications structure linking internal and external customers
- Implement a center-wide internal training program

The AFIWC is engaged in a myriad of activities supporting its role as the Air Force information warfare executive agent. The center provides information warfare services to the warfighter in contingencies and exercises through quantitative analysis, modeling and simulation, database and technical expertise in communication and computer security. The reputation of the AFIWC as the premier DOD IW organization is reflected through the outstanding performance of a diverse mission base.

2.0 REQUIREMENTS DOCUMENT SUMMARY

This document establishes the vision for a multi-tiered approach to development, demonstration and deployment of various database and applications software components supporting requirements for the production, maintenance and dissemination of information supporting the Information Warfare component of Intelligence Preparation of the Battlespace (IW/IPB).

3.0 AFIWC/IOA DIVISION BACKGROUND

The IO Analysis Division, Information Operations Directorate, Air Force Information Warfare Center (AFIWC/IOA) is responsible for supplying USAF components with the Information Warfare component of Intelligence Preparation of the Battlespace (IW/IPB). In this role, AFIWC/IOA performs a variety of multi-source intelligence analyses supporting USAF operations and acquisition communities. AFIWC/IOA, as tasked by USAF PMD and formal DOD production requirement, is responsible for development and maintenance of the Functional Networks, Signals and Equipment Parametric components of the Modernized Integrated Data Base (MIDB), multi-source analysis of target area for

critical node identification and targeting recommendations, and SIGINT and computer threat vulnerabilities assessments. AFIWC/IOA, as tasked by USAF PMD 1039(8), also serves as the Air Force representative to the MIDB Program Management Board. AFIWC/IOA is wholly responsible for system configuration management and control on both locally owned and DOD-shared databases within the division. This statement of requirement identifies undeveloped components of the information architecture required by AFIWC/IO to properly accomplish its mission.

3.1 CONSTANT WEB (CW)

The Deputy Chief of Staff for Intelligence, Headquarters U.S. Air Force (HQ USAF/IN) delegated the implementation of programmatic support for USAF Command and Control Warfare support to Headquarters Air Intelligence Agency (HQ AIA), and its executive agent, the Air Force Information Warfare Center (AFIWC). Within the AFIWC, the IO Analysis Division (AFIWC/IOA), is responsible for the acquisition, production, maintenance and dissemination of C3 information supporting IW/EW operations. CW information is maintained within DIA's national general military intelligence database, MIDB. AFIWC/IOA maintains the USAF "master" MIDB, and is connected to the national data replication ring connecting DIA with each Unified Command Joint Intelligence/Analysis Center.

3.2 SENSOR HARVEST (SH)

In post DESERT STORM analysis, a general officer steering group recognized the need for a database to support C2W planning and targeting . This evolved into an IW Target Analysis Support product called SENSOR HARVEST. SENSOR HARVEST is an IW country study-based product used for planning and execution of PSYOP, Military Deception, Electronic Warfare, Physical Attack, and Information Attack. It is applicable to strategic and tactical mission areas.

3.3 JOINT THREAT INCIDENT DATABASE (JTID)

The JTID is the first attempt to categorize threat types based on information derived from potentially hostile activity identified by the Air Force Computer Emergency Response Team (AFCERT). Our analysts combine unclassified information, derived through unique open-source research processes with known intelligence to develop a historical perspective of aggressive activity. This information is then used to identify trends and patterns of hostile actions to include aggressive Internet protocol addresses, hacking tools and methods, success and failure rates, and victim sites.

3.4 SIGINT/ELECTRONIC THREAT ANALYSIS (SETA)

Threat exists not only from the exploitation of our computer network vulnerabilities, but there is also a significant threat to our communications infrastructure. Our adversaries are exceptionally skilled in detecting changes in U.S. military Tempo of Operations and procedures, through daily monitoring of U.S. rapid deployment forces. Our threat

assessments provide the status of foreign reconnaissance efforts against U.S. military forces, as well as detailed information on U.S. systems and capabilities most susceptible to hostile targeting. Knowledge of our adversaries' collection capabilities provide our commanders with the tools to effectively employ their war fighting assets undetected and out of harms way. Additionally, this comprehensive assessment of our adversaries' collection capabilities can be used as a guide to effectively employ our own electronic combat assets to prevent intercept of our critical command and control communication-electronic transmissions.

3.5 CENTER-WIDE REQUIREMENTS MANAGEMENT (CRM)

The AFIWC/IOA collection requirements system aids in filling the information gap. Once an intelligence need is realized, our analysts search requirement databases to find what intelligence already exists. If an existing requirement does not meet analysts' needs, or does not exist, our analysts use the collection requirements system to update or produce a new requirement to register the need for information through one or multiple source disciplines (i.e., SIGINT, HUMINT, Measurement and Signature Intelligence MASINT, and Imagery Intelligence IMINT). Once the intelligence is collected, the information is sent back to the customer. If AFIWC analysts deem the information to only partially satisfy the initial requirement, the cycle is repeated.

3.6 ADDITIONAL IOA DIVISION CAPABILITIES/RESPONSIBILITIES

- Data Replication (Sybase)
- Intelink C2W Network Analysis (IC2WNA)
- MicroWeb
- Data Kinetix
- Information Warfare Portal
- IW/C2W Space
- Stand-Alone Product Generation (SPG)
- Change Management System (CMS)

4.0 GENERAL REQUIREMENTS

The environment envisioned for operations support within AFIWC/IO will include:

4.1 INTEGRATED INFORMATION PROCESSING, DISPLAY AND MAINTENANCE:

A common interface to unique production and maintenance components is required to provide IO analysts with consistency of information and applications flow. Components include, but are not limited to Constant Web, Sensor Harvest, Joint Threat Incident Database; Computer Threat Analysis Tools; SIGINT/Electronic Threat Assessment; MIDB; IW/C2W/Space; Electronic Warfare Integrated Reprogramming (EWIR), Vintage Harvest, ELINT Parameter Limits (EPL), Links and Nodes, SPIRIT, Intelink Command

and Control Warfare Network Analysis (IC2WNA); Data Kinetix (DK); Stand-Alone Product Generation (SPG); MicroWeb; Change Management System (CMS). Development of common support modules within a DOD-compliant architecture must be designed and developed through an approved configuration management process from Software Development Plan (SDP). "Logical View" integration of existing data repositories (RDBMS, flat file, graphics, text, imagery) within the AFIWC, as defined by AFIWC/IOA to include:

- Standardized "look and feel" amongst/between components
- Intuitive flow between/among various data repositories
- Data normalization

4.1.1 DATA BASE DEVELOPMENT:

Database design/development activities must:

4.1.1.1 Be based upon analysis of existing functional capabilities of each production application as well as information display requirements identified but not implemented. This analysis will include all information defined by the Constant Web, Sensor Harvest and Sensor Beam data plans/dictionaries. Be consistent with, and compliant with to the extent possible, the Modernized Integrated Data Base (MIDB) data standards, naming conventions and logical rules.

4.1.1.2 Allow for storage of textual, digital imagery, and graphical information within a common environment, and will include integration with the Common Mapping Applications Programming Interface (CMAPI).

4.1.1.3 Support compartmentalization of data, based on classification/caveats.

4.1.1.4 Be consistent with approved DOD standard data modeling efforts.

4.1.2 APPLICATIONS SOFTWARE DEVELOPMENT:

Applications software developed for AFIWC/IOA must:

4.1.2.1 Allow both manual and automated data creation and maintenance to support both local and deployed IO/IW analysis efforts, to include critical node analysis and target nomination, at multiple security levels, in both U.S.-only and coalition operations environments.

4.1.2.2 Support general intelligence analysis functions by internal and external users.

4.1.2.3 Support manual and automated quality assurance functions.

4.1.2.4 Include integration of GOTS/COTS graphic applications into the data production/maintenance environment supporting analytic data maintenance requirements.

4.1.2.5 Consider INTELINK connectivity/data transport mechanisms, including the automated application of HyperText Mark-up Language (HTML), eXtended Markup Language (XML), JAVA, and other emerging technologies.

4.1.2.6 Include Import and Export (data exchange) modules supporting a variety of customer data requirements, to include:

1. MicroWeb
2. Theater Battle Management Core System (TBMCS)
3. Global Command and Control System – Maritime (GCCS-M)
4. Global Command and Control System – Integrated Imagery & Intelligence (GCCS-I3)
5. Improved Many on Many (IMOM)
6. Air Force Mission Support System (AFMSS)
7. Joint Mission Planning System (JMPS)
8. Information Warfare Planning Capability (IWPC)
9. Joint Targeting Toolbox (JTT)
10. Adversary
11. TelScope
12. DIODE
13. CMAPI and Oilstock map graphic applications tool set
14. Special and/or one-time Customer Requirements/Requests

4.2 INFORMATION WARFARE OPERATIONS TEMPLATES

Support rapid analysis and IW recommendation requirements of potential strategies and/or components/ functions of Information Warfare to include detailed assessments of IW strategies, gathering and software implementation of OPLAN objective information and development of "templates".

4.3 C3/C4 (TECHNOLOGY) TEMPLATES

Analytic resources are not available to provide the appropriate level of information detail required for successful IW strategy implementation on a potential worldwide basis. Alleviate the burden on limited analytic resources by providing templates to support identification of available technology within a given target area. These templates will support the information gathering and capabilities assessments required for basic analytic assessments of IW strategies.

4.4 INTEGRATION/MODELING OF IO/IW INFORMATION BASED ON TEMPLATE TECHNOLOGIES

Integrate resultant assessments generated by IW and technology templates into an IW recommendation package.

4.5 ANALYST SUPPORT TOOLS

Develop and/or integrate analytic support capabilities including, but not limited to message parsing, automated database correlation/update, data mining, knowledge discovery and management, and collaboration.

4.6 CAPABILITIES/TECHNOLOGIES ASSESSMENTS

Conduct research, analysis and demonstration of new and emerging technologies that are, or may be, relevant to the Information Dominance mission of the AFIWC. Provide recommendations for integration of emerging government and contractor technologies.

4.7 PROTOTYPE DEVELOPMENT

Develop prototype activities in support of new/enhanced capabilities for AFIWC/IOA functional requirements. Include design, develop, implement, testing and demonstration. Develop plan(s) and major milestones for insertion into an operational environment. These prototype activities shall be accomplished on as required basis.

4.7.1 SUPPORT OF NEW USER FUNCTIONAL REQUIREMENTS

May include data base design activities (logical and physical), applications software design and development, or technology insertion activities (document, demonstrate).

4.7.2 DOCUMENTATION

Document features, design/architecture and user assistance, as specified/dictated by each individual prototype activity.

4.7.3 DATA EXCHANGE

Automated data exchange applications between data repositories and computer simulation models

4.7.4 DATA MODELING

Data modeling in support of new/enhanced IO/IW requirements and transition of data from existing environment(s) to the UNIX environment. Work includes implementing any approved changes to the logical and physical structures of the databases.

4.7.4.1 Relational Data Base Management System(s) (RDBMS), Object Oriented Data Base Management System(s) (OODBMS)

4.7.4.2 Logical and physical modeling in compliance with existing data models for MIDB

4.7.4.3 Analysis and design recommendations for updates to the database design as required to implement new capabilities.

4.7.4.4 Implementation plans (schedule, strategy) for accomplishing data base design and applications upgrades while maintaining existing capabilities baseline(s)

4.8 SYSTEMS ENGINEERING

Communications network(s) architecture, design, integration and maintenance to include:

a) Verification of vendor licenses

b) Recommendation for changes/upgrades

c) Traffic/Load analyses in support of enhanced network component allocation/design

d) Network /communications configuration, systems test/validation, data base administration, workstation configuration (to include hardware/software version control).

e) Applications software modifications and enhancements. Change management, resource allocation and scheduling will be prioritized and authorized by AFIWC/IO.

4.8.1 DATABASE/INFORMATION STANDARDS

Monitor and analyze the on-going design and development progress of the national migration systems for development of national standards and potential impacts to AFIWC/IOA initiatives. This monitoring and analysis shall consist of the following: attending and participating in various technical reviews and working groups; reviewing

available interface control documentation, and documenting potential issues and proposed strategies for solution.

4.8.2 CONFIGURATION MANAGEMENT

Maintain and enhance configuration management (CM) processes for all software development activities, both contractor and government, within AFIWC/IOA programs. Establish and maintain development, test and production baselines in accordance with the government-approved CM process. Coordinate, evaluate, prioritize and schedule updates to baselines. Administer software and database baseline media library.

4.8.3 INTEGRATION OF NEW HARDWARE/SOFTWARE CAPABILITIES AND/OR BASELINES

a) Analyze new/proposed technologies/capabilities. Include considerations of national migration systems impacts, interface control requirements, impacts on functional analysis capabilities.

b) Provide recommendations for integration strategy(s)

c) Implement designated integration strategy(s)

d) Engineering assistance as required for maintenance, modifications

4.9 CAPABILITIES/TECHNOLOGY INSERTION/INTEGRATION

At government discretion, technology demonstrations will be accomplished either directly through AFIWC/IO or under the auspices of the AIA Technology Demonstration Center. Demonstration(s) shall include:

a) Present system capabilities to operational users in a well-structured and planned manner. Demonstrations shall consist of the following topics:

1) an initial introduction that describes the scenario setting, and highlights system functionality that is to be demonstrated.

2) a script of demonstration capabilities.

3) feedback sessions for gathering comments.

4) potential implementations for the next demonstration. This material shall consist of either overhead slides or easy-to-assemble storyboard presentations of future screen displays and system functionality.

b) Record the operational user feedback, such as comments and correspondence obtained from personnel witnessing the demonstration, and place under internal

configuration control. User comments shall be incorporated into a future prototype. Methods of recording feedback shall include:

1) taking notes to capture the comments as they are made during the presentation.

2) accumulating, categorizing, and tracking the comments after system demonstration.

c) Demonstrate interfaces to external systems as required.

4.10 CONFIGURATION MANAGEMENT

Maintain and enhance IOA's Change Management System (CMS), which provides the ability to identify, analyze, prioritize and track requirements levied against IOA by both internal and external customers. Enhancements will include items as identified, submitted and approved through existing configuration management processes.

4.11 IW/IPB INFORMATION PORTAL

Design and develop a seamless, "operations-oriented" interface to textual, database, imagery, graphical and/or multi-media information. Developed applications must be available for implementation either as "stand-alone" applications, within an applications suite, and within an on-line web-based "Intelink" environment. Applications software development in support of external consumers of AFIWC/IOA shall include:

a) Remote user access to local applications

b) Data export/import applications

c) Complete, pre-compiled, executable applications for delivery to external, non-remote users

d) On-site support at user locations as required

e) MicroWeb: PC-based C2W Operations Support, known as MicroWeb. Developed applications software will:

1) support deployed IO/IW analysis efforts, to include Battle Damage Assessment and Uncorrelated Intelligence Data processing.

2) support intelligence analysis functions by external users.

3) include Import and Export (data exchange) modules supporting data feed to/from MIDB and the Compass Call Mission Support Facility, Blocks II and III..

4) include integration of GOTS/COTS graphic applications

5.0 SOFTWARE MAINTENANCE

Provide maintenance support for all software within the AFIWC/IOA environment as follows:

5.1.1 BASELINE SOFTWARE MAINTENANCE

Provide engineering support to maintain and enhance the AFIWC/IOA baseline architecture by identifying, correcting, testing and documenting the resolution of problems. Maintain an operational copy of AFIWC/IOA baseline system(s) for use in software implementation. In addition, maintain all software that is added to the AFIWC/IOA configuration baseline(s).

5.1.2 CHANGE REQUESTS

Routine changes or enhancements to hardware or software environment must be analyzed, prioritized and scheduled. This task requires development of appropriate processes to perform such assessment and provide the Government a work plan for each change request. Each work plan shall include the following:

a) The chronological time and man-hours required to accomplish the work (this includes designing, coding, testing, documenting, and delivering the product to the Government).

b) Software modules affected and the percentage of each module involved.

c) Documentation affected.

d) GFE computer requirements (such as lead site testing).

e) Development milestones

5.1.2.1 Provide each work plan to the Government within two (2) working days of receipt of those CRs judged by the Government to be critical to continued AFIWC/IOA operations, and within five (5) working days for all others.

5.1.2.2 Upon Government approval of the work plan design, develop, integrate, test and deliver software with appropriate documentation.

5.1.3 PERFORM DATA BASE STRUCTURE MAINTENANCE

Make any approved changes to the logical and physical design structures of locally maintained AFIWC/IOA data base(s). Such changes will first be approved through the

configuration management process established within AFIWC/IOA prior to adding to the baseline.

5.1.4 COTS SOFTWARE MAINTENANCE

As upgrades to COTS software are released by vendors, such upgrades must be assessed for impact to the AFIWC environment. Changes will first be approved through the configuration management process established prior to adding to the baseline. Upon Government approval, apply the upgrades to the AFIWC environment.

5.1.5 MAINTENANCE TESTING

Conduct acceptance testing, including regression testing, on all new maintenance releases and CRs to ensure that the changed software meets requirements and does not adversely impact existing baselines and interfaces. Include development of Maintenance Test Plan/Procedures, an installation plan and a Version Description Document.

5.1.5.1 Maintenance Releases: Resolve software problems through corrective action under CM procedures. Software maintenance releases encompassing all previous changes must be developed and provided for testing and distribution.

5.1.6 MAINTAIN ENHANCEMENTS

Develop and implement software enhancements through the standard corrective action process described in the CM Plan.

5.1.7 EXTERNAL INTERFACES

Perform an evaluation and assessment for any request for change. Provide maintenance required for continued AFIWC/IOA software interface with external systems. This will include changes in message formats, data content, or protocols that may effect AFIWC/IOA interface(s) software.

5.2 WORKING GROUPS

IO/IW User groups (semi-annual) and Technical Exchange Meetings (monthly) will be the primary focal points for discussion and coordination with users of AFIWC/IOA information. All the myriad groups identified by the AFIWC/IO are candidates for attendance.

Databases for the 21st Century II (DB21 II):
Information, Intelligence, and Information Warfare (I2/IW)
ANNEX II:
DAWS/DMFE/IET REQUIREMENTS DOCUMENT

1.0 GENERAL REQUIREMENTS:

The environment envisioned for operations support with DAWS/DMFE/IET will include:

1.1 SOFTWARE MAINTENANCE. Provide maintenance support for all software within the DAWS/DMFE/IET environment as follows:

1.1.1 BASELINE SOFTWARE MAINTENANCE. Provide engineering support to maintain and enhance the baseline architecture by identifying, correcting, testing and documenting the resolution of problems. Maintain an operational copy of DAWS/DMFE/IET baseline system(s) for use in software implementation. In addition, maintain all software that is added to the DAWS/DMFE/IET configuration baseline(s).

1.1.2 CHANGE REQUESTS (CRs). Routine changes or enhancements to hardware or software environment must be analyzed, prioritized and scheduled. This work requires development of appropriate processes to perform such assessment and provide the Government a work plan for each change request. Each work plan shall include the following:

- The chronological time and man-hours required to accomplish the work (this includes designing, coding, testing, documenting, and delivering the product to the Government).

- Software modules affected and the percentage of each module involved.

- Documentation affected.

- GFE computer requirements (such as lead site testing).

- Development milestones

1.1.2.1 Provide each work plan to the Government within two (2) working days of receipt of those CRs judged by the Government to be critical to continued DAWS/DMFE/IET operations, and within five (5) working days for all others.

1.1.2.2 Upon Government approval of the work plan design, develop, integrate, test and deliver software with appropriate documentation.

1.1.3 PERFORM DATA BASE STRUCTURE MAINTENANCE. Make any approved changes to the logical and physical design structures of DAWS/DMFE/IET data base(s). Such changes will first be approved through the configuration management process established prior to adding to the baseline.

1.1.4 COTS SOFTWARE MAINTENANCE. As upgrades to COTS software are released by vendors, such upgrades must be assessed for impact to the DAWS/DMFE/IET environment. Changes will first be approved through the configuration management process established prior to adding to the baseline. Upon Government approval, apply the upgrades to the environment.

1.1.5 MAINTENANCE TESTING. Conduct acceptance testing, including regression testing, on all new maintenance releases and CRs to ensure that the changed software meets requirements and does not adversely impact existing baselines and interfaces. Include development of Maintenance Test Plan/Procedures, an installation plan and a Version Description Document.

1.1.6 MAINTENANCE RELEASES. Resolve software problems through corrective action under CM procedures. Software maintenance releases encompassing all previous changes must be developed and provided for testing and distribution.

1.1.7 MAINTAIN ENHANCEMENTS. Develop and implement software enhancements through the standard corrective action process described in the CM Plan.

1.1.8 EXTERNAL INTERFACES. Perform an evaluation and assessment for any request for change. Provide maintenance required for continued DAWS/DMFE/IET software interface with external systems. This will include changes in message formats, data content, or protocols that may effect interface(s) software.

1.2 WORKING GROUPS. DMS User groups (semi-annual) and Technical Exchange Meetings (monthly) will be the primary focal points for discussion and coordination with users of DAWS/DMFE/IET information.

1.3 DATABASE DEVELOPMENT. Database design/development activities must:

- Be based upon analysis of existing functional capabilities of each application as well as information display requirements identified but not implemented. This analysis will include all information defined by data plans/dictionaries. Be consistent with, and compliant with to the extent possible, data standards, naming conventions and logical rules.

- Allow for storage of textual messages, attachments, digital imagery, and graphical information within a common environment.

- Support compartmentalization of data, based on classification/caveats.

- Be consistent with approved DOD standard data modeling efforts.

1.4 DATABASE/INFORMATION STANDARDS. Monitor and analyze the on-going design and development progress of the national migration systems for development of national standards and potential impacts to DAWS/DMFE/IET initiatives. This monitoring and analysis shall consist of the following: attending and participating in various technical reviews and working groups; reviewing available interface control documentation, and documenting potential issues and proposed strategies for solution.

1.5 APPLICATIONS SOFTWARE DEVELOPMENT. Applications software developed for must:

- Allow both manual and automated data creation and maintenance to support both local and deployed message analysis efforts, to include multiple security levels, in both U.S.-only and coalition operations environments.

- Support general message analysis functions by internal and external users.

- Support manual and automated quality assurance functions.

- Include integration of GOTS/COTS applications into the data production/ maintenance environment supporting analytic data maintenance requirements.

- Consider INTELINK, SIPRNET, NIPRNET and DMS connectivity/data transport mechanisms, including the automated application of Hyper-Text Mark-up Language (HTML), eXtended Markup Language (XML), JAVA, and other emerging technologies.

- Include Import and Export (data exchange) modules supporting a variety of customer data requirements

1.6 ANALYST SUPPORT TOOLS. Develop and/or integrate analytic support capabilities including, but not limited to message parsing, automated database

correlation/update, data mining, knowledge discovery and management, and collaboration.

1.7 CAPABILITIES/TECHNOLOGIES ASSESSMENTS. Conduct research, analysis and demonstration of new and emerging technologies that are, or may be, relevant to the DAWS/DMFE/IET. Provide recommendations for integration of emerging government and contractor technologies.

1.8 SUPPORT OF NEW USER FUNCTIONAL REQUIREMENTS. May include data base design activities (logical and physical), applications software design and development, or technology insertion activities (document, demonstrate).

1.9 DOCUMENTATION. Document features, designs/architectures and user assistance or familiarization.

1.10 DATA EXCHANGE. Automated data exchange applications between data repositories and analysis tools.

1.11 SYSTEMS ENGINEERING. Communications network(s) architecture, design, integration and maintenance to include:

- Verification of vendor licenses
- Recommendation for changes/upgrades
- Traffic/Load analyses in support of enhanced network component allocation/design
- Network /communications configuration, systems test/validation, data base administration, workstation configuration (to include hardware/software version control).
- Applications software modifications and enhancements.

1.12 CONFIGURATION MANAGEMENT. Maintain and enhance Configuration Management (CM) processes for all software development activities within

DAWS/DMFE/IET programs. Establish and maintain development, test and production baselines in accordance with the government-approved CM process. Coordinate, evaluate, prioritize and schedule updates to baselines. Administer software and database baseline media library.

1.13 INTEGRATION OF NEW HARDWARE/SOFTWARE CAPABILITIES AND/OR BASELINES. Analyze new/proposed technologies/capabilities. Include considerations of national migration systems impacts, interface control requirements, impacts on functional analysis capabilities.

- Provide recommendations for integration strategy(s)
- Implement designated integration strategy(s)
- Engineering assistance as required for maintenance, modifications

1.14 CAPABILITIES/TECHNOLOGY INSERTION/INTEGRATION. Technology demonstrations shall present system capabilities to operational users in a well-structured and planned manner. Demonstrations shall consist of the following topics:

- An initial introduction that describes the scenario setting, and highlights system functionality that is to be demonstrated.
- A script of demonstration capabilities.
- Feedback sessions for gathering comments.
- Potential implementations for the next demonstration. This material shall consist of either overhead slides or easy-to-assemble storyboard presentations of future screen displays and system functionality.
- Record the operational user feedback, such as comments and correspondence obtained from personnel witnessing the demonstration, and place under

internal configuration control. User comments shall be incorporated into a future prototype. Methods of recording feedback shall include:

- Taking notes to capture the comments as they are made during the presentation.

- Accumulating, categorizing, and tracking the comments after system demonstration.

- Demonstrate interfaces to external systems as required.

- Document all feedback from the demonstrations as Software Change Requests and implement the software changes according to government specified priorities.

1.15 IMPROVE DAWS/DMFE/IET GRAPHICAL USER INTERFACE (GUI). Provide an enhanced and simplified Graphical User Interface (GUI) for the DAWS/DMFE/IET. Evaluate the current process the user must go through to generate a message and identify methods for simplifying the process.

1.15.1 Update the DAWS/DMFE/IET Software User Manual to reflect all GUI changes and enhancements.

1.16 WEB/BROWSER BASED DAWS/DMFE/IET PRODUCTS. Develop a simple web capable/browser based method for requesting DAWS/DMFE/IET products via the network. At a minimum, this interface will provide online users with:

- A list of available product generation capabilities that the user can select and run.
- A list of previously generated products that the user can download.

- A simple mechanism to profile a product.
- Provide both product push and pull capabilities. For Push, allow a user to specify a location on the network where a finished product should be stored. For Pull,

provide the user with notification of when their product is ready and a location from which to retrieve it.

1.16.1 Develop an online help function for the simple web interface and update the DAWS/DMFE/IET SUM to include this capability.

1.17 CD ROM BASED PATCH CAPABILITY. Develop a CD ROM based patch capability for future DAWS/DMFE/IET releases and upgrades. This capability will permit the application of single or multiple patches to an existing installation without forcing the need to do a full DAWS/DMFE/IET replacement. Include the capability to have both the latest release of the full DAWS/DMFE/IET product as well as a set of patches on each distributed CD. Provide a patch utility on the CD that automatically determines the user's current patch level of DAWS/DMFE/IET and apply additional patches accordingly. Update the DAWS/DMFE/IET software installation manual.

1.18 SOFTWARE TEST AND VALIDATION. Test and validate the functionality of all software developed or modified

1.19 ON-SITE SOWTWARE INSTALLATION SUPPORT. Provide onsite software installation support as required for both the DAWS/DMFE and the Information Extraction Tool (IET) toolsets.

1.20 TELEPHONE SUPPORT. Provide telephone support as required for both DAWS/DMFE and IET.

1.21 MANAGEMENT AND PROGRAM SUPPORT. Provide Program Management Support in order to accomplish the following:

1.21.1 Continually determine the state of the effort and report progress toward accomplishment of contract requirements. Report man-hour expenditures monthly.

1.21.2 Conduct oral presentations at such times and places designated in the contract schedule. Provide status of technical progress made to date in performance of the contract during presentations.

1.21.3 Provide a schedule of activities and milestones at the start of the effort.

1.22 SOFTWARE. Design, develop, evaluate, document, and deliver all software in accordance with the requirements of the Databases for the 21st Century (DB21) II Statement of Work (SOW) and the following:

1.22.1 Deliver all computer software developed under this effort as source and object (executable) code on electronic media, including commented source listings.

1.22.2 Delivered software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation.

1.22.3 For all software purchased or licensed for use as a component of the software to be delivered, arrangements shall be made for licensing and maintenance agreements to be transferred to the Government upon the completion of this effort.

1.22.4 All information technology items must be Year 2000 compliant, or non-compliant items must be upgraded to be Year 2000 compliant upon delivery. Year 2000 compliant means information technology that accurately processes data/time data (including but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

Databases for the 21st Century II (DB21 II):
Information, Intelligence, and Information Warfare (I2/IW)
ANNEX III:
IFE/IFEA/IFEB/IFEC/IFEDTECHNICAL AREAS

I. Core Technology Areas: IDIQ Orders may be issued against IFE, IFEA, IFEB, IFEC or IFED technical areas encompassing Global Awareness, Information Exploitation, Information Fusion or Global Information Base, including:

A. Information Fusion
B. Knowledge Base Technology
C. Information Extraction
D. Information Data Handling
E. Mass Storage & Retrieval
F. Image/Video Exploitation
G. Speech/Audio Processing
H. SIGINT Exploitation
I. Targeting/Weaponeering/Combat Assessment

II. Supporting Technologies, Programs and Initiatives: Orders may also be issued against these IFE/IFEA/IFEB/IFEC/IFED supporting technologies, programs and initiatives:

A. Global Awareness and the Joint Battlesphere Initiative (JBI)

B. Precision Engagement and Full Dimensional Aerospace Protection by advancing the state of the art in intelligence, surveillance and reconnaissance exploitation capabilities.

C. The processing, storage, fusion, and dissemination of both real-time and stored information in support of all battlespace participants.

D. The performance of selected acquisition programs for low-volume, limited quantity systems for the intelligence community.

E. Technology integration to provide a common operating picture to dynamic planning and to the data warehouse functions. Data collection operation to improve the quality of targeting. Develop capabilities to differentiate potential targets as friend, foe, or neutral, in sufficient time, with high confidence, and at the requisite range, to support weapons release and engagement decisions.

F. Steganography and digital watermarking technologies. Signals intelligence technology (SIGINT) under the Defense Cryptological Program, including baseline technology COMINT and Proforma for application to new efforts for signal assurance/identification and user recognition. Joint Reserve Intelligence Facility (JRIF)-SPACE-INFO OPS, Test and Evaluation capability in the AFRL/Rome JRIF.

G. The evaluation and transition of advanced database technologies and implementations (such as XML and XML Schema), concept based retrieval, information extraction, knowledge management, information sharing strategies, and information access, retrieval and storage.

Databases for the 21st Century II (DB21 II):

Information, Intelligence, and Information Warfare (I2/IW)

ANNEX IV:

AFRL/IFGB TECHNICAL AREAS

IDIQ Orders may be issued against any of the following IFGB technical areas:

A. CyberForensics
B. Secure System Engineering
C. Automated Intrusion Detection Development
D. Data Hiding
E. Boundary Control
F. Dynamic Coalitions
G. Secure Mobile Code
H. Fault Tolerant Network Technique Development
I. Active Network Response/Information Resiliency
J. Signature Analysis
K. Anomaly Detection
L. Network Management-Intrusion Control Integration
M. Data Mining
N. Strategic Intrusion Assessment
O. Formal Methods
P. Firewall Policies/Tools
Q. Damage Assessment/Recovery
R. Data Bridging and Wrapper Technology

Databases for the 21st Century II (DB21 II):

Information, Intelligence, and Information Warfare (I2/IW)

ANNEX V:

AFIWC TECHNICAL AREAS

IDIQ Orders may be issued against any of the following AFIWC technical areas:

A. Data, Data Structures, and Data Architectures
   1. IW/C2W Vulnerabilities, Targeting and Related
   2. IW Country Studies
   3. IW Target Folders
   4. Functional C3 Networks
   5. Computer Threat
   6. SIGINT/Electronic Threat
   7. Space IW
   8. Battlefield Visualization
   9. MIDB
   10. Intelligence Preparation of the Battlespace
   11. Information Warfare Portal

B. Databases
   1. Sensor Harvest
   2. Sensor Beam
   3. Constant Web
   4. MIDB
   5. IW/C2W Space
   6. Joint Threat Incident Database
   7. SIGINT/Electronic Threat Database
   8. Vintage Harvest
   9. Space Database

10. Links & Nodes
11. SPIRIT
12. Electronic Warfare Integrated Reprogramming
13. IOPT/IWPC
14. Change Management System

C. Applications
    1. MIDB Maintenance
    2. Sensor Harvest Maintenance
    3. Joint Threat Incident Database Maintenance
    4. Computer Threat Analysis Tools Maintenance
    5. Intelink
        a. IC2WNA
        b. Sensor Harvest
        c. JTID
        d. CTAT
    6. Data/Product Exchange
        a. SPG
        b. DEX
        c. Sybase BCP
        d. Oracle Dump/Restore
    7. IW Space Analysis Maintenance
    8. MicroWeb II (and follow-on)
    9. Middleware
        a. Data Kinetix
        b. Sybase Enterprise Portal
    10. Information Operations Analytic Capabilities

D. Products
    1. MIDB
    2. Sensor Harvest (Intelink, CD-ROM)
    3. JTID (Intelink)
    4. MicroWeb
    5. IMOM

E. Operations Planning Tools
    1. IOPT/IWPC
    2. IO/IW Targeting

3. IO/IW Planning, Modeling, and Analysis

F. Analyst/User/Customer Tools

G. Systems

1. Administration and Maintenance

H. Architectures

1. Data and Information
2. Database
3. Client/Server
4. System
5. Enterprise

I. Configuration Management

1. Change Management System

Databases for the 21st Century II (DB21 II):

Information, Intelligence, and Information Warfare (I2/IW)

ANNEX VI:

DAWS/DMFE/IET TECHNICAL AREAS

IDIQ Orders may be issued against any of the following DAWS/DMFE/IET technical areas:

A. Message Generation

1. Message validation
2. Message templates
3. Legal value hot key
4. Message Security
5. Message Addressing
6. Message Sectioning
7. Message Definition
8. Message Formatting and Typing
9. Message Editing/Modification
10. Message Error Handling
11. Message Release
12. Message Routing
13. Message Attachments
14. Message Generation Defaults
15. Browser – Web enabling

B. Message Handling

1. Message Error Handling
2. Message Profiling and Editing
3. Message Statistics
4. Message Validation
5. Message Sorting
6. Message Parsing
7. Message Release
8. Message Security
9. Message Addressing and Lists

10. Message Dissemination and Status
11. Message Storage and Retrieval
12. Message Tracking
13. Message Display Configurability
14. Message Statistics and Status
15. Message Identification, Tracking, and Status
16. Message Queuing
17. Message Search
18. Message Notification
19. Message Query and Saved Queries
20. Message Keywords and Highlighting
21. Message Enclosures
22. Message Virus Checking
23. Message Display
24. Message Formatting
25. E-Mail Services
26. Browser – Web enabling

C. System Administration

1. Message Error Handling
2. Create and Maintain Users
3. Create and Maintain User Permissions
4. Create and Maintain Classes and Objects
5. Create and Maintain Templates
6. System Security and Auditing
7. System Reporting
8. System Data Bases
9. System Access and Editing
10. System Configuration
11. Create and Maintain Message Queues
12. System Print
13. System Timeouts
14. Message Access and Intercept
15. Browser – Web enabling

D. General Services

1. Message Text Handling

2. System and Message Directory Services
3. System Configuration and Installation Scripts
4. JITF Testing
5. AFDI Compliance
6. DII COE Compliance
7. Y2K Certification and documentation
8. System Auto- print and Auto- log services
9. System Backup and Recovery
10. System Warnings and Thresholds
11. System Software and Upgrades
12. Message Archival and Retrieval
13. System and Message Meta-Tagging
14. Message Query Generation, Save and Retrieval; Public and Private
15. System and User Defaults
16. System Documentation
17. System Security and Access Restrictions
18. System Printing and Banners
19. Message Type Formats
20. Profile Editing
21. Geo-Spatial display and profiling
22. System and Message Timeline Analysis
23. System Classification
24. System Services Automation
25. System Limitations and Performance
26. Multi DBMS Operations
27. Multi Operating System Support
28. Browser – Web enabling